Melissa A. Huelsman, WSBA #30935
Law Offices of Melissa A. Huelsman, P.S.
705 Second Avenue, Suite 606
Seattle, Washington 98104
(206) 447-0103 – Telephone
(206) 673-8220 – Facsimile
mhuelsman@predatorylendinglaw.com

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

NOEL U. WOODARD, individually and on behalf of all others similarly situated, Plaintiff, v. CENTURYLINK, INC., Defendant.	NO. **CLASS ACTION COMPLAINT FOR DAMAGES (with Jury Demand)**

Plaintiff NOEL U. WOODARD ("Plaintiff" or "Woodard") brings this action individually, and on behalf of all others similarly situated, by and through counsel, and against Defendant CENTURYLINK, INC. ("CenturyLink" or "Defendant"), and hereby alleges as follows:

INTRODUCTION

1. CenturyLink is a global technology company "that provides residential, business, and enterprise customers with a variety of products and services, including internet, phone, cable TV, cloud solutions, and security."[1]

2. CenturyLink maintains personally identifiable information ("PII") relative to its customers, including customers' names, email addresses, phone numbers, physical addresses, and other account-specific information and the contents of their email correspondence (*e.g.*, account numbers, logs of communications with CenturyLink, etc.).[2]

3. As of at least November 17, 2018, CenturyLink stored some or all of the PII it maintained in a single database (the "Database").[3]

4. On September 15, 2019, security researcher Bob Diachenko ("Diachenko") discovered that the Database "was made publicly available such that no authentication was required to access it" (the "Data Breach").[4] Although "Diachenko notified CenturyLink" of the Data Breach that same day, "the database had already been exposed for many months"—approximately 10 months in total.[5] "This would have given malicious parties more than ample time to use the data in various schemes."[6]

5. At the time the Data Breach was discovered, the Database contained more than 2.8 million records of consumer PII in total.[7]

---

[1] Comparitech, *CenturyLink Customer Details Exposed Online, 2.8 Million Records Leaked*, available at: https://www.comparitech.com/blog/information-security/centurylink-data-leak/.

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*

6. CenturyLink's failures to adopt, implement, maintain, and enforce proper data security policies and procedures resulted in Plaintiff's and other similarly situated individuals' PII being improperly exposed and disclosed to unauthorized third parties.

7. Plaintiff brings this suit on behalf of herself and a Class of similarly situated individuals against CenturyLink for its failure to protect their PII.

PARTIES

8. Plaintiff Woodard is a natural person and resident and citizen of King County, Washington.

9. Defendant CenturyLink is a Louisiana corporation with a principal place of business located at 100 CenturyLink Drive, Monroe, Louisiana 71203.

JURISDICTION AND VENUE

10. This Court has personal jurisdiction over Defendant because it regularly conducts business in Washington and has sufficient minimum contacts in Washington. Defendant has intentionally availed itself of this jurisdiction by marketing and selling products and services in Washington.

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy in this matter exceeds $5,000,000, there are 100 or more members of the putative Class, and members of the putative Class are from different states than Defendant. Indeed, according to a recent news article, the Database contained records for at least "hundreds of thousands" of individuals.[8]

12. Venue is proper in this District, pursuant to 28 U.S.C. § 1391 because a substantial portion of the transactions and occurrences relevant to this action took place in this District.

[8] *Id.*

DAMAGES FROM DATA BREACHES

13. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

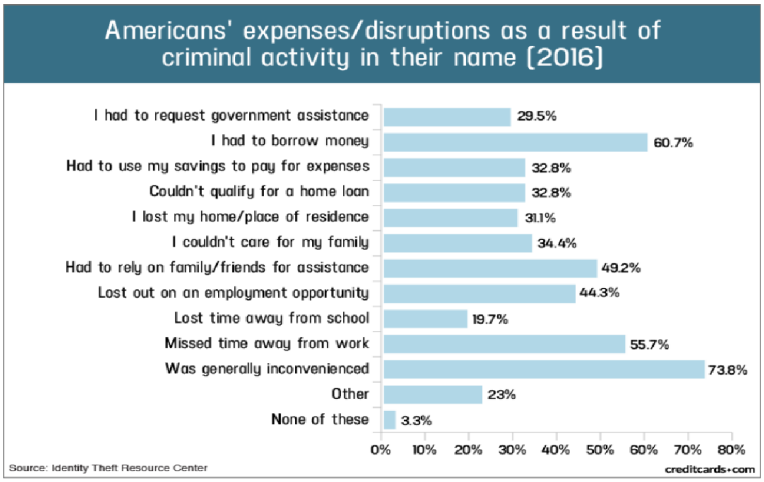
14. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

15. Identity thieves can also use stolen PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services in the victim's name, access various other accounts, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

16. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal information:[10]

[9] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2, June 2007, available at: https://www.gao.gov/new.items/d07737.pdf.

[10] Jason Steele, *Credit Card and ID Theft Statistics*, October 24, 2017, available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



17. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See, GAO Report, p. 29.

18. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. "Consumers sometimes discover their credentials have been stolen only after fraudsters use their personal medical ID to impersonate them and obtain health services. When unpaid bills are sent on to debt collectors, they track down fraud victims and seek payment."[11]

19. Thus, there is a strong probability that entire batches of stolen information have

[11] Reuters, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, available at: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

been dumped on the black market, and are yet to be dumped on the black market, meaning Defendant's customers are at an increased risk of fraud and identity theft for years into the future.

THE DATA BREACH

20. Plaintiff and Class members entrusted their PII with CenturyLink in connection with the technology services provided to them by CenturyLink.

21. Although the Database contained sensitive PII, Defendant failed to implement and adopt reasonable procedures to ensure that Plaintiff's and Class members' PII would be protected from access by malicious third parties. The Database contained a security flaw that permitted anyone to access Plaintiff's and Class members' PII.

22. On information and belief, third parties did, in fact, access and obtain Plaintiff's and Class members' PII from the Database as a direct result of the security flaw.

23. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

24. Plaintiff and members of the Class have or will suffer actual injury as a direct result of the Data Breach. In addition to financial fraud and damage to their credit, many victims have or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Contacting their financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

j. Resetting other accounts that were compromised;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

25. Plaintiff and Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

26. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have also suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

27. The aforementioned harms to Plaintiff and Class members was compounded by the fact that, despite becoming aware of the Data Breach on September 15, 2019, CenturyLink did not inform Plaintiff and Class members until approximately October 18, 2019. This gave malicious third parties additional time to utilize Plaintiff's and Class members' PII for nefarious purposes, and deprived Plaintiff and Class members of the ability to take remedial measures sooner.

FACTS RELEVANT TO PLAINTIFF

Plaintiff Noel Woodard

28. On information and belief, one or more third-parties accessed and stole Plaintiff's PII stored on the Database as a direct result of the Data Breach. On information and belief, that third party (or third parties), used Plaintiff's stolen PII for a variety of malicious purposes.

29. Plaintiff received an email message from CenturyLink on October 18, 2019, stating:

> Dear Valued Customer,
>
> Your business is important to us, and we take your information privacy seriously. Recently, we became aware of an information security incident involving a CenturyLink third-party vendor. As a result, information about customers was inadvertently made publicly accessible online, including name, address, phone number, email address and CenturyLink account number. Our initial investigation has determined that no financial, password or similar sensitive information was involved.
>
> **What steps has CenturyLink taken?**
> As soon as we became aware of a security issue potentially exposing your contact information, CenturyLink mobilized an internal team led by our Chief Security Officer. We will continue to work to implement security measures to prevent similar incidents and have taken additional steps to safeguard your information.
>
> **What should you do to protect yourself?**
> As noted above, this incident did not involve sensitive information, but there are measures that you can take to improve protection of your data. We've provided a list of suggestions for you on our website at news.centurylink.com/customer-information, including tips regarding how to identify fraudulent attempts to contact you via email or phone, good password practices, and resetting devices routinely to make sure software is updated.
>
> This site also includes FAQs and ways to contact CenturyLink for additional information. You can also call us at 888-595-7750.
>
> We know these types of incidents can be concerning or even frustrating. We appreciate the trust you put in us by sharing your information with us, and we are committed to making our security measures as strong as possible to safeguard that information. We sincerely apologize for any inconvenience this issue may cause. Thank you for being a CenturyLink customer.
>
> Sincerely,

Maxine Moreau
CenturyLink
President, Consumer Markets

30. Plaintiff has an email account with CenturyLink. By obtaining access to Plaintiff's CenturyLink email account, third parties were able to obtain access to Plaintiff's other online accounts. For example:

a. On November 17, 2019, Woodard received a notice from her MyIDCare that one of her identity monitoring services has a new notification;

b. On November 23, 2019, Woodard received a phishing email notifying her that her primary email account that was linked to her CenturyLink account was exposed to a data breach on October 16, 2019;

c. On November 24, 2019, Woodard received a notification from Firefox Monitor notifying her that her primary email account that was linked to her CenturyLink account was exposed to a data breach as of November 22, 2019;

d. On December 19, 2019, Woodard received a notification from McAfee that she had a new identity alert.

31. Prior to receiving any of the correspondence described above, Plaintiff had not previously received notice of an identity alert and/or phishing emails.

32. Plaintiff was particularly concerned about the phishing emails as these "phishing" emails are particularly advanced because they contain personalized information which makes them almost indistinguishable from legitimate emails.

33. All of the foregoing unusual and unauthorized activity relative to Woodard's various online accounts have one common denominator: the CenturyLink email and billing accounts. Moreover, Woodard does not use public Wi-Fi and utilizes data protection software on all of her electronic devices, which further supports the conclusion that this unusual and unauthorized activity was the result of the Data Breach.

34. As a result of the unusual and unauthorized activity, Woodard took and continues to take measures to ensure her identity has not been stolen and her accounts have not been compromised. Woodard has been required to place secondary control measures on several of her accounts to ensure that she does not lose access once again. As a direct and proximate result of Defendant's actions and inactions, Plaintiff has incurred, and will continue to incur, costs and expenses in the form of the time spent, and time she will continue to spend, dealing with the theft of her PII.

35. As a direct and proximate result of Defendant's conduct, Woodard has also been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft because her CenturyLink email account contains messages with even more sensitive PII (such as credit card numbers, financial information, tax information, etc.).

36. In addition, Woodard has suffered anxiety and emotional distress as a direct and proximate result of Defendant's failures to keep her PII secure.

37. Woodard was further harmed by Defendant's failure to timely inform her of the Data Breach, as it allowed malicious third parties to continue to utilize her stolen PII for nefarious means based on the continued notifications of her identity being compromised.

CLASS ALLEGATIONS

38. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P. 23, on behalf of a nationwide class of similarly situated individuals and entities (the "Class"), defined as follows:

> All individuals and entities whose PII was stored in the Database during the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees,

officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

39. **Numerosity and Ascertainability**: Upon information and belief, the Class is comprised of hundreds of thousands of individuals and entities,[12] and is so numerous that joinder of all members is impracticable. While the exact number of Class members is presently unknown and can only be ascertained through discovery, Class members can be identified through Defendant's records or by other means.

40. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiff and members of the Class which predominate over any individual issues, including:

a. Whether Defendant adequately protected Plaintiff's and Class members' PII;

b. Whether Defendant adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the Database;

c. Whether Defendant properly trained employees to prevent the unauthorized access to the Database;

d. Whether Defendant failed to promptly notify customers of the Data Breach;

e. Whether Defendant owed a duty to Plaintiff and Class members to safeguard and protect their PII;

f. Whether Defendant breached its duty to protect Plaintiff's and Class members' PII by its failure to adopt, implement, and maintain reasonable policies and procedures to prevent the unauthorized access to the Database; and

[12] Comparitech, *CenturyLink Customer Details Exposed Online, 2.8 Million Records Leaked*, available at: https://www.comparitech.com/blog/information-security/centurylink-data-leak/ (noting that the Database contained PII for "hundreds of thousands" of individuals).

g. Whether Defendant is liable for the damages suffered by Plaintiff and Class members as a result of the theft of their PII, as well as the measure and amount of Plaintiff's and Class members' damages.

41. **Typicality**: Plaintiff's claims are typical of the claims of the Class. All claims are based on the same legal and factual issues. Plaintiff and each of the Class members were customers of CenturyLink, provided their PII to Defendant, entrusted Defendant with their PII, and had their PII accessed from the Database by malicious actors. Defendant's conduct was uniform to Plaintiff and all Class members.

42. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to those of the Class, and Defendant has no defense unique to Plaintiff.

43. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiff's and Class members' claims are manageable.

COUNT I
Negligence

44. Plaintiff repeats and re-allege the allegations of paragraphs 1–43 with the same force and effect as though fully set forth herein.

45. Defendant knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class members' PII and the importance of adequate security. Defendant was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

46. Defendant had a common law duty to prevent foreseeable harm to those whose PII they were entrusted with. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of the failure of Defendant to adopt, implement, and maintain reasonable security measures so that Plaintiff's and Class members' PII would not be publicly accessible in an online Database.

47. Defendant had a special relationship with Plaintiff and Class members. Defendant was entrusted with Plaintiff's and Class members' PII, and Defendant was in a position to protect that PII from public exposure.

48. Defendant's duties also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' PII. Various FTC publications and data security breach orders further form the basis for Defendant's duties.

49. Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' PII in its possession so that it would not come within the possession, access, or control of unauthorized persons.

50. More specifically, Defendant's duties included, *inter alia*, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting PII, including policies, procedures, and security measures to ensure that PII is not accessible online in unsecured storage servers and are password-protected;

b. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of individuals' PII with entities that failed to adopt, implement, and maintain policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

c. Adopt, implement, and maintain reasonable policies and procedures to ensure that they are sharing individuals' PII only with entities that have

adopted, implemented, and maintained policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

d. Properly train employees to protect individuals' PII; and

e. Adopt, implement, and maintain processes to quickly detect data breaches and/or security flaws, and to promptly act on warnings about data breaches and/or security flaws.

51. Defendant breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' PII so that their PII would not come within the possession, access, or control of unauthorized persons.

52. Defendant acted with reckless disregard for the security of Plaintiff's and Class members' PII because Defendant knew or should have known that its data security practices were not adequate to safeguard the PII that it collected and stored, and because Defendant failed to promptly detect the Data Breach.

53. As a result of Defendant's conduct, Plaintiff and Class members have suffered, and will continue to suffer, actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and rectifying unauthorized access to their various other accounts; and increased risk of future harm. Further, Plaintiff and Class members have suffered, and will continue to suffer, other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

54. Defendant also had an affirmative duty to notify Plaintiff and Class members in the most expedient time possible if it was, or is reasonably believed to have been, subject to a Data Breach, so that Plaintiff and Class members could take appropriate and timely measures to mitigate damages, protect against adverse consequences, and thwart future incidents of identity theft.

55. Defendant breached its duty to timely inform Plaintiff and Class members of the Data Breach because it became aware of the Data Breach on September 15, 2019, but did not inform Plaintiff and Class members of the Security Flaw until approximately October 18, 2019.

56. As a result of Defendant's failure to provide timely notification to Plaintiff and Class members of the Data Breach, Defendant prevented Plaintiff and Class members from taking timely and proactive steps to secure their financial data, bank accounts, and other accounts where their personal and financial information could be used for fraudulent purposes, including identity theft.

COUNT II
Violation of the Consumer Fraud and Deceptive Trade Practices Acts of the Various States and District of Columbia

57. Plaintiff repeats and re-allege the allegations of paragraphs 1–43 with the same force and effect as though fully set forth herein.

58. Plaintiff brings this Count individually, and on behalf of the Class for violations of the respective statutory consumer protection laws, as follows:

A. the Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8–19–1, *et seq*.;

B. the Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, *et seq*.;

C. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq*.;

D. the Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, *et seq*.;

E. the California Unfair Competition Law, Cal.Bus. & Prof. Code §§17200, *et seq*. and 17500 *et seq*.;

F. the California Consumers Legal Remedies Act, Civil Code §§1750, *et seq*.;

G. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq*.;

H. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110a, *et seq*.;

I. the Delaware Consumer Fraud Act, 6 Del. C. § 2511, *et seq*.;

J. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq*.;

K. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, *et seq*.;

L. the Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq*.;

M. the Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq*.;

N. the Idaho Consumer Protection Act, I.C. § 48-601, *et seq*.;

O. the Ohio Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 *et seq*.;

P. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq*.;

Q. The Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq*.;

R. the Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq*.;

S. the Kentucky Consumer Protection Act, KRS 367.110, *et seq*.;

T. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq*.;

U. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq*.;

V. the Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, *et seq*.;

W. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq*.;

X. the Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq*.;

Y. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68, *et seq*.;

Z. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq*.;

AA. the Missouri Merchandising Practices Act, V.A.M.S. § 407.010, *et seq*.;

BB. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq*.;

CC. the Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, *et seq*.;

DD. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq*.;

EE. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, *et seq*.;

FF. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq*.;

GG. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq*.;

HH. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, *et seq*.;

II. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq*.;

JJ. the North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, *et seq*.;

KK. the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq*.;

LL. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq*.;

MM. the Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq*.;

NN. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq*.;

OO. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), *et seq*.;

PP. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, *et seq*.;

QQ. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq*.;

RR. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq*.;

SS. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq*.;

TT. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq*.;

UU. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq*.;

VV. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq*.;

WW. the Washington Consumer Protection Act, RCWA 19.86.010, *et seq*.;

XX. the West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, *et seq*.;

YY. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100, *et seq*.; and

ZZ. the Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq*.

59. Defendant engaged in unfair and deceptive acts or practices when it accepted and stored Plaintiff's and Class members' PII and then failed to adopt, implement, and maintain reasonable measures to protect that PII.

60. Defendant represented to Plaintiff and Class members that their PII would be safeguarded from access by unauthorized individuals, and that it would inform Plaintiff and Class members of any threats to the security of their PII.

61. For example, on its website, CenturyLink represents that it "takes immense precautions in monitoring, preventing, and identifying fraudulent behavior related to its website;"[13] states that "when malicious activity is detected on your account, we provide web and email (when available) notifications for your protection;"[14] and markets a variety of data security products.[15] CenturyLink also states that when it shares PII with other companies, it "require[s] these companies to use our information only for the purposes we specify and to keep it safe and confidential." In addition, CenturyLink's privacy policy states that: "Only CenturyLink employees, agents, service providers and other businesses we work and share information with and who have a legitimate business purpose are authorized to access customer information. This

[13] CenturyLink, *Online Security*, available at: https://www.centurylink.com/aboutus/legal/online-security.html.

[14] CenturyLink, *CenturyLink Consumer Internet Protection Program*, available at: https://www.centurylink.com/home/support/internetprotection/.

[15] *See,e.g.*, CenturyLink, *Enhanced Cybersecurity Services*, available at: https://www.centurylink.com/business/resources/product-finder.html#security; CenturyLink, *Cloud Security*, available at: https://www.centurylink.com/business/security/cloud.html; CenturyLink, *Email Security*, available at: https://www.centurylink.com/business/security/email-security.html.

access is strictly defined (often involving password controlled access and other security controls) and subject to policies and contracts requiring confidential treatment of the information…We use secure technologies to transfer sensitive information and comply with a variety of industry standards, and federal and state laws regarding the protection of customer information."[16] CenturyLink's privacy policy also states that "We have security measures in place to protect against [unauthorized] access."[17]

62. For the reasons set forth above, the foregoing representations were false.

63. Defendant intended for Plaintiff and the members of the Class to rely upon its misrepresentations and omissions, and Plaintiff and Class members did, in fact, rely upon these misrepresentations and omissions.

64. Had Plaintiff and Class members known that Defendant did not have adequate measures in place to protect their PII, they would not have entrusted their PII to Defendant and/or would have required Defendant to adopt, implement, and maintain adequate security measures, including measures to ensure the information would not be provided to third parties that did not have adequate measures in place, before providing their PII.

65. The above-described deceptive and unfair acts and practices were used or employed in the conduct of trade or commerce.

66. The above-described deceptive and unfair acts offend public policy and cause substantial injury to consumers.

67. Defendant's conduct implicates consumer protection concerns as its data security practices affect the public generally.

---

[16] CenturyLink, *Complete Privacy Policy*, available at: https://www.centurylink.com/aboutus/legal/privacy-policy/privacy-policy-complete.html.

[17] *Id*.

68. As a result of Defendant's conduct, Plaintiff and Class members have suffered, and will continue to suffer, actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and rectifying unauthorized access to their various other accounts; and increased risk of future harm. Further, Plaintiff and Class members have suffered, and will continue to suffer, other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

69. Plaintiff and Class members have suffered damages as a direct and proximate result of Defendant's unfair and unconscionable commercial practices. These substantial injuries outweigh any benefit to consumers or competition that may result from Defendant's unfair practices.

COUNT III
Breach of Contract

70. Plaintiff repeats and re-allege the allegations of paragraphs 1–43 with the same force and effect as though fully set forth herein.

71. Defendant and Plaintiff and Class members entered into an agreement that included a promise by Defendant that Plaintiff's and Class members' PII would be safeguarded from access by unauthorized individuals, and that Defendant would inform Plaintiff and Class members of any threats to the security of their PII.

72. For example, on its website, Defendant represents that it "takes immense precautions in monitoring, preventing, and identifying fraudulent behavior related to its website;"[18] states that "when malicious activity is detected on your account, we provide web and

[18] CenturyLink, *Online Security*, available at: https://www.centurylink.com/aboutus/legal/online-security.html.

email (when available) notifications for your protection;"[19] and markets a variety of data security products.[20] Defendant also states that when it shares PII with other companies, it "require[s] these companies to use our information only for the purposes we specify and to keep it safe and confidential." In addition, Defendant's privacy policy states that: "Only CenturyLink employees, agents, service providers and other businesses we work and share information with and who have a legitimate business purpose are authorized to access customer information. This access is strictly defined (often involving password controlled access and other security controls) and subject to policies and contracts requiring confidential treatment of the information…We use secure technologies to transfer sensitive information and comply with a variety of industry standards, and federal and state laws regarding the protection of customer information."[21] Defendant's privacy policy also states that "We have security measures in place to protect against [unauthorized] access."[22]

73. Defendant breached these contractual obligations which allowed the Data Breach to occur.

74. Defendant's data security obligations were part of the benefit of the bargain with Plaintiff and Class members. Plaintiff and Class members paid money for Defendant's products and services, a portion of which was for the bargained for data security practices.

---

[19] CenturyLink, *CenturyLink Consumer Internet Protection Program*, available at: https://www.centurylink.com/home/support/internetprotection/.

[20] *See,e.g.*, CenturyLink, *Enhanced Cybersecurity Services*, available at: https://www.centurylink.com/business/resources/product-finder.html#security; CenturyLink, *Cloud Security*, available at: https://www.centurylink.com/business/security/cloud.html; CenturyLink, *Email Security*, available at: https://www.centurylink.com/business/security/email-security.html.

[21] CenturyLink, *Complete Privacy Policy*, available at: https://www.centurylink.com/aboutus/legal/privacy-policy/privacy-policy-complete.html.

[22] *Id*.

75. Plaintiff and Class members suffered damages as a result of Defendant's breach of its contractual obligations, including its privacy policy,

76. As a result of Defendant's breach of contract and the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and rectifying unauthorized access to their various other accounts; and increased risk of future harm. Further, Plaintiff and Class members have suffered, and will continue to suffer, other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

77. Plaintiff and Class members have also been deprived of the benefit of the bargain in amounts they paid Defendant for promised reasonable and adequate data security practices that Defendant failed to perform and provide. In addition to the damages described above, Plaintiff and the Class members seek damages in the amount of their lost benefit of the bargain, which includes amounts Plaintiff and the other Class members paid to Defendant for the provision of adequate and reasonable data security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff NOEL U. WOODARD, individually, and on behalf of all others similarly situated, prays for an Order as follows:

A. Finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. Designating Plaintiff as representative of the Class, and the undersigned counsel as Class Counsel;

C. Entering judgment in favor of Plaintiff and the Class, and against Defendant;

D. Awarding Plaintiff and the Class actual damages, punitive damages, and all other forms of available relief;

E. Entering an injunction requiring Defendant to adopt, implement, and maintain adequate security measures to protect Plaintiff's and Class members' PII;

F. Awarding Plaintiff's Counsel their attorney's fees and costs, including interest thereon, as allowed or required by law; and

G. Granting all such further and other relief as the Court deems just and appropriate.

JURY DEMAND

Plaintiff demands a trial by jury on all counts so triable.

Respectfully Submitted,

By: */s/ Melissa A. Huelsman*
Law Offices of Melissa A. Huelsman, P.S.
705 Second Avenue, Suite 606
Seattle, Washington 98104
(206) 447-0103 telephone
(206) 673-8220 facsimile
mhuelsman@predatorylendinglaw.com
paralegal@predatorylendinglaw.com

Marc E. Dann (0039425) (*Pro hac vice anticipated)*
DANNLAW
P.O. Box. 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiff and the putative Class